Common ports/services and how to use them

Port X - Service unknown

If you have a port open with unkown service you can do this to find out which service it might be.

```
nmap -d 192.168.19.244 8000
```

Port 21 - FTP

Connect to the ftp-server to enumerate software and version

```
 ftp 192.168.1.101
nc 192.168.1.101 21
```

Many ftp-servers allow anonymous users. These might be misconfigured and give too much access, and it might also be necessary for certain exploits to work. So always try to log in with `anonymous:anonymous`.

Remember the binary and ascii mode!

If you upload a binary file you have to put the ftp-server in binary mode, otherwise the file will become corrupted and you will not be able to use it! The same for text-files. Use ascii mode for them! You just write **binary** and **ascii** to switch mode.

Port 22 - SSH

SSH is such an old and fundamental technology so most modern version are quite hardened. You can find out the version of the SSH either but scanning it with nmap or by connecting with it using `nc`.

```
nc 192.168.1.10 22
```

It returnes something like this: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu1

This banner is defined in RFC4253, in chapter 4.2 Protocol Version Exchange. http://www.openssh.com/txt/rfc4253.txt The protocol-version string should be defined like this: `SSH-protoversion-softwareversion SP comments CR LF` Where comments is optional. And SP means space, and CR (carriege return) and LF (Line feed) So basically the comments should be separated by a space.

Port 23 - Telnet

Telnet is considered insecure mainly because it does not encrypt its traffic. Also a quick search in exploit-db will show that there are various RCE-vulnerabilities on different versions. Might be worth checking out.

Brute force it

You can also brute force it like this:

```
hydra -l root -P /root/SecLists/Passwords/10_million_password_list_top_100.txt 192.168.1.101 telnet
```

Port 25 - SMTP

SMTP is a server to server service. The user receives or sends emails using IMAP or POP3. Those messages are then routed to the SMTP-server which communicates the email to another server. The SMTP-server has a database with all emails that can receive or send emails. We can use SMTP to query that database for possible email-addresses. Notice that we cannot retrieve any emails from SMTP. We can only send emails.

Here are the possible commands

```
 HELO -
EHLO - Extended SMTP.
STARTTLS - SMTP communicted over unencrypted protocol. By starting TLS-session we encrypt the traffic.
RCPT - Address of the recipient.
DATA - Starts the transfer of the message contents.
RSET - Used to abort the current email transaction.
MAIL - Specifies the email address of the sender.
QUIT - Closes the connection.
HELP - Asks for the help screen.
AUTH - Used to authenticate the client to the server.
VRFY - Asks the server to verify is the email user's mailbox exists.
```

Manually

We can use this service to find out which usernames are in the database. This can be done in the following way.

```
 nc 192.168.1.103 25

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY root
252 2.0.0 root
VRFY roooooot
550 5.1.1 <roooooot>: Recipient address rejected: User unknown in local recipient table
```

Here we have managed to identify the user `root`. But `roooooot` was rejected.

`VRFY`, `EXPN` and `RCPT` can be used to identify users.

Telnet is a bit more friendly some times. So always use that too

```
telnet 10.11.1.229 25
```

Automatized

This process can of course be automatized

Check for commands

```
nmap -script smtp-commands.nse 192.168.1.101
```

smtp-user-enum

The command will look like this. `-M` for mode. `-U` for userlist. `-t` for target

```
smtp-user-enum -M VRFY -U /root/sectools/SecLists/Usernames/Names/names.txt -t 192.168.1.103
```

```
 Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /root/sectools/SecLists/Usernames/Names/names.txt
Target count ............. 1
Username count ........... 8607
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Sun Jun 19 11:04:59 2016 #########
192.168.1.103: Bin exists
192.168.1.103: Irc exists
192.168.1.103: Mail exists
192.168.1.103: Man exists
192.168.1.103: Sys exists
######## Scan completed at Sun Jun 19 11:06:51 2016 #########
5 results.

8607 queries in 112 seconds (76.8 queries / sec)
```

Metasploit

I can also be done using metasploit

```
 msf > use auxiliary/scanner/smtp/smtp_enum
msf auxiliary(smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                               Required  Description
   ----       ---------------                                               --------  -----------
   RHOSTS                                                                   yes       The target address range or CIDR identifier
   RPORT      25                                                            yes       The target port
   THREADS    1                                                             yes       The number of concurrent threads
   UNIXONLY   true                                                          yes       Skip Microsoft bannered servers when testing
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable use
```

Here are the documentations for SMTP https://cr.yp.to/smtp/vrfy.html

http://null-byte.wonderhowto.com/how-to/hack-like-pro-extract-email-addresses-from-smtp-server-0160814/

http://www.dummies.com/how-to/content/smtp-hacks-and-how-to-guard-against-them.html

http://pentestmonkey.net/tools/user-enumeration/smtp-user-enum

https://pentestlab.wordpress.com/2012/11/20/smtp-user-enumeration/

Port 69 - TFTP

This is a ftp-server but it is using UDP.

Port 80 - HTTP

Info about web-vulnerabilities can be found in the next chapter `HTTP - Web Vulnerabilities`.

We usually just think of vulnerabilities on the http-interface, the web page, when we think of port 80. But with `.htaccess` we are able to password protect certain directories. If that is the case we can brute force that the following way.

Password protect directory with htaccess

Step 1

Create a directory that you want to password-protect. Create .htaccess tile inside that directory. Content of .htaccess:

```
 AuthType Basic
AuthName "Password Protected Area"
AuthUserFile /var/www/html/test/.htpasswd
Require valid-user
```

Create .htpasswd file

```
 htpasswd -cb .htpasswd test admin
service apache2 restart
```

This will now create a file called .htpasswd with the user: test and the password: admin

If the directory does not display a login-prompt, you might have to change the **apache2.conf** file. To this:

```
 <Directory /var/www/html/test>
    AllowOverride AuthConfig
</Directory>
```

Brute force it

Now that we know how this works we can try to brute force it with medusa.

```
 medusa -h 192.168.1.101 -u admin -P wordlist.txt -M http -m DIR:/test -T 10
```

Port 88 - Kerberos

Kerberos is a protocol that is used for network authentication. Different versions are used by *nix and Windows. But if you see a machine with port 88 open you can be fairly certain that it is a Windows Domain Controller.

If you already have a login to a user of that domain you might be able to escalate that privilege.

Check out: MS14-068

Port 110 - Pop3

This service is used for fetching emails on a email server. So the server that has this port open is probably an email-server, and other clients on the network (or outside) access this server to fetch their emails.

```
 telnet 192.168.1.105 110
USER pelle@192.168.1.105
PASS admin

# List all emails
list

# Retrive email number 5, for example
retr 5
```

Port 111 - Rpcbind

RFC: 1833

Rpcbind can help us look for NFS-shares. So look out for nfs. Obtain list of services running with RPC:

```
 rpcbind -p 192.168.1.101
```

Port 119 - NNTP

Network time protocol. It is used synchronize time. If a machine is running this server it might work as a server for synchronizing time. So other machines query this machine for the exact time.

An attacker could use this to change the time. Which might cause denial of service and all around havoc.

Port 135 - MSRPC

This is the windows rpc-port. https://en.wikipedia.org/wiki/Microsoft_RPC

Enumerate

```
 nmap 192.168.0.101 --script=msrpc-enum
```

```
 msf > use exploit/windows/dcerpc/ms03_026_dcom
```

Port 139 and 445- SMB/Samba shares

Samba is a service that enables the user to share files with other machines. It has interoperatibility, which means that it can share stuff between linux and windows systems. A windows user will just see an icon for a folder that contains some files. Even though the folder and files really exists on a linux-server.

Connecting

For linux-users you can log in to the smb-share using smbclient, like this:

```
 smbclient -L 192.168.1.102
smbclient //192.168.1.106/tmp
smbclient \\\\192.168.1.105\\ipc$ -U john
smbclient //192.168.1.105/ipc$ -U john
```

If you don't provide any password, just click enter, the server might show you the different shares and version of the server. This can be useful information for looking for exploits. There are tons of exploits for smb.

So smb, for a linux-user, is pretty much like and ftp or a nfs.

Here is a good guide for how to configure samba:
https://help.ubuntu.com/community/How%20to%20Create%20a%20Network%20Share%20Via%20Samba%20Via%20CLI%20(Command-

line%20interface/Linux%20Terminal)%20-%20Uncomplicated,%20Simple%20and%20Brief%20Way!

```
mount -t cifs -o user=USERNAME,sec=ntlm,dir_mode=0077 "//10.10.10.10/My Share" /mnt/cifs
```

Connectin with PSExec

If you have credentials you can use psexec you easily log in. You can either use the standalone binary or the metasploit module.

```
use exploit/windows/smb/psexec
```

Scanning with nmap

Scanning for smb with Nmap

```
nmap -p 139,445 192.168.1.1/24
```

There are several NSE scripts that can be useful, for example:

```
ls -l /usr/share/nmap/scripts/smb*
```

```
-rw-r--r-- 1 root root  45K Jan 24  2016 /usr/share/nmap/scripts/smb-brute.nse
-rw-r--r-- 1 root root 4.8K Jan 24  2016 /usr/share/nmap/scripts/smb-enum-domains.nse
-rw-r--r-- 1 root root 5.8K Jan 24  2016 /usr/share/nmap/scripts/smb-enum-groups.nse
-rw-r--r-- 1 root root 7.9K Jan 24  2016 /usr/share/nmap/scripts/smb-enum-processes.nse
-rw-r--r-- 1 root root  12K Jan 24  2016 /usr/share/nmap/scripts/smb-enum-sessions.nse
-rw-r--r-- 1 root root 6.8K Jan 24  2016 /usr/share/nmap/scripts/smb-enum-shares.nse
-rw-r--r-- 1 root root  13K Jan 24  2016 /usr/share/nmap/scripts/smb-enum-users.nse
-rw-r--r-- 1 root root 1.7K Jan 24  2016 /usr/share/nmap/scripts/smb-flood.nse
-rw-r--r-- 1 root root 7.3K Jan 24  2016 /usr/share/nmap/scripts/smb-ls.nse
-rw-r--r-- 1 root root 8.6K Jan 24  2016 /usr/share/nmap/scripts/smb-mbenum.nse
-rw-r--r-- 1 root root 7.0K Jan 24  2016 /usr/share/nmap/scripts/smb-os-discovery.nse
-rw-r--r-- 1 root root 5.0K Jan 24  2016 /usr/share/nmap/scripts/smb-print-text.nse
-rw-r--r-- 1 root root  63K Jan 24  2016 /usr/share/nmap/scripts/smb-psexec.nse
-rw-r--r-- 1 root root 5.0K Jan 24  2016 /usr/share/nmap/scripts/smb-security-mode.nse
-rw-r--r-- 1 root root 2.4K Jan 24  2016 /usr/share/nmap/scripts/smb-server-stats.nse
-rw-r--r-- 1 root root  14K Jan 24  2016 /usr/share/nmap/scripts/smb-system-info.nse
-rw-r--r-- 1 root root 1.5K Jan 24  2016 /usr/share/nmap/scripts/smbv2-enabled.nse
-rw-r--r-- 1 root root 7.5K Jan 24  2016 /usr/share/nmap/scripts/smb-vuln-conficker.nse
-rw-r--r-- 1 root root 6.5K Jan 24  2016 /usr/share/nmap/scripts/smb-vuln-cve2009-3103.nse
-rw-r--r-- 1 root root 6.5K Jan 24  2016 /usr/share/nmap/scripts/smb-vuln-ms06-025.nse
-rw-r--r-- 1 root root 5.4K Jan 24  2016 /usr/share/nmap/scripts/smb-vuln-ms07-029.nse
-rw-r--r-- 1 root root 5.7K Jan 24  2016 /usr/share/nmap/scripts/smb-vuln-ms08-067.nse
-rw-r--r-- 1 root root 5.5K Jan 24  2016 /usr/share/nmap/scripts/smb-vuln-ms10-054.nse
-rw-r--r-- 1 root root 7.2K Jan 24  2016 /usr/share/nmap/scripts/smb-vuln-ms10-061.nse
-rw-r--r-- 1 root root 4.5K Jan 24  2016 /usr/share/nmap/scripts/smb-vuln-regsvc-dos.nse
```

```
nmap -p 139,445 192.168.1.1/24 --script smb-enum-shares.nse smb-os-discovery.nse
```

nbtscan

```
nbtscan -r 192.168.1.1/24
```

It can be a bit buggy sometimes so run it several times to make sure it found all users.

Enum4linux

Enum4linux can be used to enumerate windows and linux machines with smb-shares.

The do all option:

```
enum4linux -a 192.168.1.120
```

For info about it ere: https://labs.portcullis.co.uk/tools/enum4linux/

rpcclient

You can also use rpcclient to enumerate the share.

Connect with a null-session. That is, without a user. This only works for older windows servers.

```
rpcclient -U "" 192.168.1.101
```

Once connected you could enter commands like

```
 srvinfo
enumdomusers
getdompwinfo
querydominfo
netshareenum
netshareenumall
```

Port 143/993 - IMAP

IMAP lets you access email stored on that server. So imagine that you are on a network at work, the emails you recieve is not stored on your computer but on a specific mail-server. So every time you look in your inbox your email-client (like outlook) fetches the emails from the mail-server using imap.

IMAP is a lot like pop3. But with IMAP you can access your email from various devices. With pop3 you can only access them from one device.

Port 993 is the secure port for IMAP.

Port 161 and 162 - SNMP

Simple Network Management Protocol

SNMP protocols 1,2 and 2c does not encrypt its traffic. So it can be intercepted to steal credentials.

SNMP is used to manage devices on a network. It has some funny terminology. For example, instead of using the word password the word community is used instead. But it is kind of the same thing. A common community-string/password is public.

You can have read-only access to the snmp.Often just with the community string `public`.

Common community strings

```
 public
private
community
```

Here is a longer list of common community strings: https://github.com/danielmiessler/SecLists/blob/master/Miscellaneous/wordlist-common-snmp-community-strings.txt

MIB - Management information base

SNMP stores all teh data in the Management Information Base. The MIB is a database that is organized as a tree. Different branches contains different information. So one branch can be username information, and another can be processes running. The "leaf" or the endpoint is the actual data. If you have read-access to the database you can read through each endpoint in the tree. This can be used with snmpwalk. It walks through the whole database tree and outputs the content.

snmpwalk

```
snmpwalk -c public -v1 192.168.1.101 #community string and which version
```

This command will output a lot of information. Way to much, and most of it will not be relevant to us and much we won't understand really. So it is better to request the info that you are interested in. Here are the locations of the stuff that we are interested in:

```
 1.3.6.1.2.1.25.1.6.0 System Processes
1.3.6.1.2.1.25.4.2.1.2 Running Programs
1.3.6.1.2.1.25.4.2.1.4 Processes Path
1.3.6.1.2.1.25.2.3.1.4 Storage Units
1.3.6.1.2.1.25.6.3.1.2 Software Name
1.3.6.1.4.1.77.1.2.25 User Accounts
1.3.6.1.2.1.6.13.1.3 TCP Local Ports
```

Now we can use this to query the data we really want.

snmpenum

snmp-check

This is a bit easier to use and with a lot prettier output.

```
snmp-check -t 192.168.1.101 -c public
```

Scan for open ports - Nmap

Since SNMP is using UDP we have to use the `-sU` flag.

```
nmap -iL ips.txt -p 161,162 -sU --open -vvv -oG snmp-nmap.txt
```

Onesixtyone

With onesixtyone you can test for open ports but also brute force community strings. I have had more success using onesixtyone than using nmap. So better use both.

```
```

Metasploit

There are a few snmp modules in metasploit that you can use. snmp_enum can show you usernames, services, and other stuff.

https://www.offensive-security.com/metasploit-unleashed/snmp-scan/

Port 199 - Smux

Port 389/636 - Ldap

Lightweight Directory Access Protocol. This port is usually used for Directories. Directory her means more like a telephone-directory rather than a folder. Ldap directory can be understood a bit like the windows registry. A database-tree. Ldap is sometimes used to store usersinformation. Ldap is used more often in corporate structure. Webapplications can use ldap for authentication. If that is the case it is possible to perform **ldap-injections** which are similar to sqlinjections.

You can sometimes access the ldap using a anonymous login, or with other words no session. This can be useful becasue you might find some valuable data, about users.

```
ldapsearch -h 192.168.1.101 -p 389 -x -b "dc=mywebsite,dc=com"
```

When a client connects to the Ldap directory it can use it to query data, or add or remove.

Port 636 is used for SSL.

There are also metasploit modules for Windows 2000 SP4 and Windows Xp SP0/SP1

Port 443 - HTTPS

Okay this is only here as a reminder to always check for SSL-vulnerabilities such as heartbleed. For more on how to exploit web-applications check out the chapter on client-side vulnerabilities.

Heartbleed

OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable OpenSSL 1.0.1g is NOT vulnerable OpenSSL 1.0.0 branch is NOT vulnerable OpenSSL 0.9.8 branch is NOT vulnerable

First we need to investigate if the https-page is vulnerable to heartbleed

We can do that the following way.

```
sudo sslscan 192.168.101.1:443
```

or using a nmap script

```
nmap -sV --script=ssl-heartbleed 192.168.101.8
```

You can exploit the vulnerability in many different ways. There is a module for it in burp suite, and metasploit also has a module for it.

```
 use auxiliary/scanner/ssl/openssl_heartbleed
set RHOSTS 192.168.101.8
set verbose true
run
```

Now you have a flow of random data, some of it might be of interest to you.

CRIME

Breach

Certificate

Read the certificate. - Does it include names that might be useful? - Correct vhost

Port 554 - RTSP

RTSP (Real Time Streaming Protocol) is a stateful protocol built on top of tcp usually used for streaming images. Many commercial IP-cameras are running on this port. They often have a GUI interface, so look out for that.

Port 587 - Submission

Outgoing smtp-port

If Postfix is run on it it could be vunerable to shellshock https://www.exploit-db.com/exploits/34896/

Port 631 - Cups

Common UNIX Printing System has become the standard for sharing printers on a linux-network. You will often see port 631 open in your priv-esc enumeration when you run `netstat`. You can log in to it here: **http://localhost:631/admin**

You authenticate with the OS-users.

Find version. Test **cups-config –version**. If this does not work surf to **http://localhost:631/printers** and see the CUPS version in the title bar of your browser.

There are vulnerabilities for it so check your searchsploit.

Port 993 - Imap Encrypted

The default port for the Imap-protocol.

Port 995 - POP3 Encrypten

Port 995 is the default port for the **Post Office Protocol**. The protocol is used for clients to connect to the server and download their emails locally. You usually see this port open on mx-servers. Servers that are meant to send and recieve email.

Related ports: 110 is the POP3 non-encrypted.

25, 465

Port 1025 - NFS or IIS

I have seen them open on windows machine. But nothing has been listening on it.

Port 1030/1032/1033/1038

I think these are used by the RPC within Windows Domains. I have found no use for them so far. But they might indicate that the target is part of a Windows domain. Not sure though.

Port 1433 - MsSQL

Default port for Microsoft SQL .

```
sqsh -S 192.168.1.101 -U sa
```

Execute commands

```
 # To execute the date command to the following after logging in
xp_cmdshell 'date'
go
```

Many o the scanning modules in metasploit requires authentication. But some do not.

```
use auxiliary/scanner/mssql/mssql_ping
```

Brute force.

```
scanner/mssql/mssql_login
```

If you have credencials look in metasploit for other modules.

Port 1521 - Oracle database

Enumeration

```
 tnscmd10g version -h 192.168.1.101
tnscmd10g status -h 192.168.1.101
```

Bruteforce the ISD

```
auxiliary/scanner/oracle/sid_brute
```

Connect to the database with `sqlplus`

References:

http://www.red-database-security.com/wp/itu2007.pdf

Ports 1748, 1754, 1808, 1809 - Oracle

These are also ports used by oracle on windows. They run Oracles **Intelligent Agent**.

Port 2049 - NFS

Network file system This is a service used so that people can access certain parts of a remote filesystem. If this is badly configured it could mean that you grant excessive access to users.

If the service is on its default port you can run this command to see what the filesystem is sharing

```
showmount -e 192.168.1.109
```

Then you can mount the filesystem to your machine using the following command

```
 mount 192.168.1.109:/ /tmp/NFS
mount -t 192.168.1.109:/ /tmp/NFS
```

Now we can go to /tmp/NFS and check out /etc/passwd, and add and remove files.

This can be used to escalate privileges if it is not correct configured. Check chapter on Linux Privilege Escalation.

Port 2100 - Oracle XML DB

There are some exploits for this, so check it out. You can use the default Oracle users to access to it. You can use the normal ftp protocol to access it.

Can be accessed through ftp. Some default passwords here: https://docs.oracle.com/cd/B10501_01/win.920/a95490/username.htm Name: Version:

Default logins: sys:sys scott:tiger

Port 3268 - globalcatLdap

Port 3306 - MySQL

Always test the following:

Username: root

Password: root

```
 mysql --host=192.168.1.101 -u root -p
mysql -h <Hostname> -u root
mysql -h <Hostname> -u root@localhost
mysql -h <Hostname> -u ""@localhost

telnet 192.168.0.101 3306
```

You will most likely see this a lot:

```
 ERROR 1130 (HY000): Host '192.168.0.101' is not allowed to connect to this MySQL server
```

This occurs because mysql is configured so that the root user is only allowed to log in from 127.0.0.1. This is a reasonable security measure put up to protect the database.

Configuration files

```
 cat /etc/my.cnf
```

http://www.cyberciti.biz/tips/how-do-i-enable-remote-access-to-mysql-database-server.html

Mysql-commands cheat sheet

http://cse.unl.edu/~sscott/ShowFiles/SQL/CheatSheet/SQLCheatSheet.html

Uploading a shell

You can also use mysql to upload a shell

Escalating privileges

If mysql is started as root you might have a chance to use it as a way to escalate your privileges.

MYSQL UDF INJECTION:

https://infamoussyn.com/2014/07/11/gaining-a-root-shell-using-mysql-user-defined-functions-and-setuid-binaries/

Finding passwords to mysql

You might gain access to a shell by uploading a reverse-shell. And then you need to escalate your privilege. One way to do that is to look into the databse and see what users and passwords that are available. Maybe someone is resuing a password?

So the first step is to find the login-credencials for the database. Those are usually found in some configuration-file oon the web-server. For example, in joomla they are found in:

```
 /var/www/html/configuration.php
```

In that file you find the

```
 <?php
class JConfig {
var $mailfrom = 'admin@example.com';
var $fromname = 'testuser';
var $sendmail = '/usr/sbin/sendmail';
var $password = 'myPassowrd1234';
var $sitename = 'test';
var $MetaDesc = 'Joomla! - the dynamic portal engine and content management system';
var $MetaKeys = 'joomla, Joomla';
var $offline_message = 'This site is down for maintenance. Please check back again soon.';
}
```

Port 3339 - Oracle web interface

Port 3389 - Remote Desktop Protocol

This is a proprietary protocol developed by windows to allow remote desktop.

Log in like this

```
rdesktop -u guest -p guest 10.11.1.5 -g 94%
```

Brute force like this

```
ncrack -vv --user Administrator -P /root/passwords.txt rdp://192.168.1.101
```

Ms12-020

This is categorized by microsoft as a RCE vulnerability. But there is no POC for it online. You can only DOS a machine using this exploit.

Port 4445 - Upnotifyp

I have not found anything here. Try connecting with netcat and visiting in browser.

Port 4555 - RSIP

I have seen this port being used by Apache James Remote Configuration.

There is an exploit for version 2.3.2

https://www.exploit-db.com/docs/40123.pdf

5060 / 5061 - SIP

- PBX - Public branch exchange

A private phone exchange, usually found inside a company for example.

- Trunk - Connects a PBX with the rest of the telephone-network.

Lync is being rebranded to Skype for business. So today it is basically the same thing.

Asterix is a software implementation of a PBX.

Session Initiation Protocol (SIP). SIP V 2.0 is standardized in RFC 3261: https://tools.ietf.org/html/rfc3261. It has since then changed a bit in other RFCs. SIP communicates over TCP/UDP and SCTP. It uses port 5060 for unencrypted traffic and 5061 for encrypted.

SIP is just phones over the IP network. - A Client is usually called a `SIP User Agent`. In order for one user agent to call another both need to listen on their ports, usually 5060 or 5061. However, how would one user that is trying to call another user know at which IP address that user is at?

Flow of a call within a domain

Step 1. Register

So the first step for a client is to send the above mentioned registration data to the registrar. So lets say that both our callers boot up their sip-phones. On boot they send their AOR and ip address to the registrar

It works like this. When a user boot up its phone/client, that client will send a message to the `Registrar`. The message contains the device Address of Record (AOA). The AOR has this format: `SIP:user@domain`. And the client will also send its contact address, ie its ip address. So it will send it like this: `sip:1003@company.com sip:192.168.11.1:5060`

Step 2. Invitation So when the userA wants to call userB, he sends an `INVITE` to the `LOCATION` service, which knows the ip address of userB. So it proxies the call to the userB.

Step 3. Response UserB picks up the phone, and his ip-address is sent through the `LOCATION` service, to UserA. So now userA has userB:s ip address.

So the fundamental components here are: Registrar service SIP registry (the database with the clients info) Location Service

Flow of a call outside of the domain

So the client registrar his AOR to his local SIP server. The SIP server, or SIP proxy, looks up the AOR for the recipient, but can't find it. So it looks at the domain: 1999@othercompany.se So it performs a lookup to othercompany.se, finds the ip-adress and the direct the INVITE to that server.

Calling a non-ip phone

So is it possible to call a non-ip phone? Yes. For that you can use a Signalling gateway. Signall protocol translator. Example of those are SS7. But you need a a translator, that translates from SIP to Public switched telephone netowkr (PSTN).

Protocol level analysis

So, let's look at exchange between two user agents/client. This is a scenario where they are on the same network and know each others ip.

```
 ALICE is calling BOB.
ALice INVITE ---->      BOB
Alice <---- 100 Trying  BOB
Alice <---- 180 Ringing BOB
Alice <---- 200 OK      BOB
Alice ACK ---->         BOB

ALICE DATA <-----> DATA BOB

Alice hangs up
Alice BYE ---->         BOB
Alice <---- 200 OK      BOB
```

Port 5357 - WSDAPI

Port 5722 - DFSR

> The Distributed File System Replication (DFSR) service is a state-based, multi-master file replication engine that automatically copies updates to files and folders between computers that are participating in a common replication group. DFSR was added in Windows Server 2003 R2.

I am not sure how what can be done with this port. But if it is open it is a sign that the machine in question might be a Domain Controller.

Port 5900 - VNC

VNC is used to get a screen for a remote host. But some of them have some exploits.

You can use vncviewer to connect to a vnc-service. Vncviewer comes built-in in Kali.

It defaults to port 5900. You do not have to set a username. VNC is run as a specific user, so when you use VNC it assumes that user. Also note that the password is not the user password on the machine. If you have dumped and cracked the user password on a machine does not mean you can use them to log in. To find the VNC password you can use the metasploit/meterpreter post exploit module that dumps VNC passwords

```
 background
use post/windows/gather/credentials/vnc
set session X
exploit
```

```
 vncviewer 192.168.1.109
```

Ctr-alt-del

If you are unable to input ctr-alt-del (kali might interpret it as input for kali).

Try `shift-ctr-alt-del`

Metasploit scanner

You can scan VNC for logins, with bruteforce.

Login scan

```
 use auxiliary/scanner/vnc/vnc_login
set rhosts 192.168.1.109
run
```

Scan for no-auth

```
 use auxiliary/scanner/vnc/vnc_none_auth
set rhosts 192.168.1.109
run
```

Port 8080

Since this port is used by many different services. They are divided like this.

Tomcat

Tomcat suffers from default passwords. There is even a module in metasploit that enumerates common tomcat passwords. And another module for exploiting it and giving you a shell.

Port 9389 -

> Active Directory Administrative Center is installed by default on Windows Server 2008 R2 and is available on Windows 7 when you install the Remote Server Administration Tools (RSAT).